UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/817,148	04/02/2004	Andrew Dellow	851963.416	1198

38106 7590 06/11/2007

SEED INTELLECTUAL PROPERTY LAW GROUP PLLC
701 FIFTH AVENUE, SUITE 5400
SEATTLE, WA 98104-7092

EXAMINER	
ALMEIDA, DEVIN E	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
06/11/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/817,148	DELLOW ET AL.	
	Examiner	Art Unit	
	Devin Almeida	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 April 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *10/18/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the papers filed 4/2/2004. Claims 1-30 were received for consideration. No preliminary amendments for the claims were filed. Currently claims 1-20 are under consideration.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on 10/18/2004 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 14 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 14 recites the limitation "the flash memory". There is insufficient antecedent basis for this limitation in the claim. For the application of art the flash memory is going to be construed as the memory.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-4, 14-17, 19-22, 24-28 and 30 are rejected under 35 U.S.C. 102(e) as being anticipated by Warren (U.S. 6,430,727). With respect to claim 1, a semiconductor integrated circuit arranged to execute application code received from a memory via external connections, comprising: a processor (see column 2 line 24-47 i.e. CPU) for executing application code from the memory (see column 2 line 24-47 i.e. memory); an internal bus (see column 2 line 24-47 i.e. bus) within the integrated circuit for providing the application code to the processor from the external connections (see column 2 line 24-47); a verifier processor (see column 2 line 24-47 i.e. CPU) arranged to receive the application code via the internal bus, wherein the verifier processor is arranged to continually process the application code using a verification function whilst the processor executes from the memory and to impair the function of the integrated circuit in the event that the application code does not satisfy the verification function (see column 2 line 24-47), and an instruction monitor arranged to monitor code requests issued by the processor and to impair the function of the circuit unless the address of the code falls within a given range (see column 2 line 24-47).

With respect to claim 2, wherein the given range is predefined and stored in an internal memory (see column 2 line 48-54).

With respect to claim 3, wherein the given range is derived by the verifier processor during a first check of the memory (see column 2 line 24-60).

With respect to claim 4, wherein the code in memory is in the form of a linked list and the given range comprises a table of linked list addresses (see column 2 line 24-60).

With respect to claim 14, wherein the verifier processor requests portions application code from the flash memory at intervals between requests by the processor for portions of the application code (see column 2 line 24-60).

With respect to claim 15, wherein the verifier processor requests portions of application code less frequent intervals than the processor (see column 2 line 24-60).

With respect to claim 16, wherein the verifier processor is arranged to request portions of application code at pseudo random times (see column 2 line 24-60).

With respect to claim 17, wherein the verifier processor is arranged to carry out read requests at a faster rate during a first check than in subsequent checks (see column 2 line 24-60).

With respect to claims 19 and 25, a semiconductor integrated circuit arranged to execute application code received from an external memory via an external connection, comprising: a processor (see column 2 line 24-47 i.e. CPU) for executing the application code from the memory (see column 2 line 24-47 i.e. memory); an internal bus (see column 2 line 24-47 i.e. bus) within the integrated circuit and connected to the processor to provide the application code to the processor from the external connections (see column 2 line 24-47); and a verifier processor (see column 2 line 24-47) arranged to

receive the application code via the internal bus, wherein the verifier processor is structured to process the application code using a verification function while the processor executes from the memory and to impede the execution of the integrated circuit if the application code does not satisfy the verification function (see column 2 line 24-47).

With respect to claims 20 and 26, an instruction monitor connected to internal bus and structured to monitor code requests issued by the processor and to impair the execution of the circuit unless the address of the code falls within a given range (see column 2 line 24-54).

With respect to claims 21 and 27, wherein the given range is derived by the verifier processor during a check of the memory (see column 2 line 24-54).

With respect to claims 22 and 28, wherein the code in memory is accessed by a linked list and the given range is stored in a table of linked list addresses (see column 2 line 24-54).

With respect to claims 24 and 30, wherein the verification processor includes: an internal processor (see column 2 line 24-47 i.e. CPU) that coordinates the processing of the application using the verification function and impairs the execution of the integrated circuit if the application code does not satisfy the verification function (see column 2 line 24-54); a code memory, coupled to the internal processor (see column 2 line 24-47 i.e. CPU); and an interface circuit that connects the internal processor with the internal bus (see column 2 line 24-47 i.e. bus).

Claims 1-4, 10-12, 14-17, 19, and 25 are rejected under 35 U.S.C. 102(e) as being anticipated by Morais (U.S. 2003/0229777). With respect to claim 1, a semiconductor integrated circuit arranged to execute application code received from a memory via external connections, comprising: a processor (see figure 2A element 202 CPU) for executing application code from the memory (see figure 2A); an internal bus within the integrated circuit for providing the application code to the processor (see figure 2A) from the external connections (see figure 2A i.e. the ROM's pins); a verifier processor (see figure 2A element 212) arranged to receive the application code (see figure 4 and paragraph 0034 i.e. running the chipset initialize code in the ROM) via the internal bus (see figure 2A), wherein the verifier processor (see figure 2A element 212) is arranged to continually process the application code using a verification function whilst the processor executes from the memory (see figure 4 and paragraph 0034-0039) and to impair the function of the integrated circuit in the event that the application code does not satisfy the verification function (see figure 4 and paragraph 0035), and an instruction monitor arranged to monitor code requests issued by the processor and to impair the function of the circuit unless the address of the code falls within a given range (see figure 4 and paragraph 0034-0039 i.e. The comparison is made in a decision step 256 to determine if the stored hash value is equal to the actual hash value that was determined. If not, the machine instructions in bootstrap code implement a step 258, which stops the boot-up process of game console).

With respect to claim 2, wherein the given range is predefined and stored in an internal memory (see paragraph 0035 i.e. also included within bootstrap code is a stored hash value that is expected hash value for preloader).

With respect to claim 3, wherein the given range is derived by the verifier processor during a first check of the memory (see paragraph 0035 i.e. accordingly, the hash value obtained by hashing the machine instructions included within preloader 230 should always remain the same, so long as preloader 230 has not been altered or or replaced with unauthorized code. In preferred embodiment, an SHA-1 one-way hash algorithm is applied to the preloader).

With respect to claim 4, wherein the code in memory is in the form of a linked list and the given range comprises a table of linked list addresses (see paragraph 0034-0035).

With respect to claim 10, wherein the verification function includes a hash function on the application code (see figure 4 and paragraph 0034-0039 i.e. The comparison is made in a decision step 256 to determine if the stored hash value is equal to the actual hash value that was determined. If not, the machine instructions in bootstrap code implement a step 258, which stops the boot-up process of game console).

With respect to claim 11, wherein the verifier processor is arranged to receive a stored secret from the memory and the verification function is a comparison of the secret and the processed application code (see figure 4 and paragraph 0034-0039 i.e. The comparison is made in a decision step 256 to determine if the stored hash value is

equal to the actual hash value that was determined. If not, the machine instructions in bootstrap code implement a step 258, which stops the boot-up process of game console).

With respect to claim 12, wherein the verification function comprises hashing the application code to produce hashed code, retrieving a signature of the code from a signature store within the memory and verifying the hashed code and signature using a public key (see figure 4 step 266).

With respect to claim 14, wherein the verifier processor requests portions application code from the flash memory at intervals between requests by the processor for portions of the application code (see paragraph 0034-0039).

With respect to claim 15, wherein the verifier processor requests portions of application code less frequent intervals than the processor (see paragraph 0034-0039).

With respect to claim 16, wherein the verifier processor is arranged to request portions of application code at pseudo random times (see paragraph 0034-0039).

With respect to claim 17, wherein the verifier processor is arranged to carry out read requests at a faster rate during a first check than in subsequent checks (see paragraph 0034-0039).

With respect to claims 19 and 25, a semiconductor integrated circuit arranged to execute application code received from an external memory via an external connection, comprising: a processor (see figure 2A element 202 CPU) for executing the application code from the memory (see figure 2A element i.e. ROM); an internal bus (see figure 2A) within the integrated circuit and connected to the processor to provide the application

code to the processor from the external connections (see figure 2A i.e. the ROM's pins); and a verifier processor arranged to receive the application code via the internal bus, wherein the verifier processor is structured to process the application code (see figure 4 and paragraph 0034 i.e. running the chipset initialize code in the ROM) using a verification function while the processor executes from the memory and to impede the execution of the integrated circuit if the application code does not satisfy the verification function (see figure 4 and paragraph 0034-0039 i.e. the comparison made in a decision step 256 to determine if the stored hash value is equal to the actual hash value that was determined. If not, the machine instructions in bootstrap code implement a step 258, which stops the boot-up process of game console).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 5-9, 13, 18, 23 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Warren (U.S. 6,430,727) in view of Harding et al (U.S. 2003/0005277). Morais and Warren teaches everything with respect to claim 4 above but with respect to claim 5, Morais does not teaches wherein the verifier processor is arranged to impair the function of the integrated circuit if the verification function is not completed for one complete cycle of the linked list within a predetermined time (see

Harding paragraph 0016). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have a timer to make sure the BIOS has finished in a certain amount of time to make sure that the BIOS is going as planned (see Harding paragraph 0016). Therefore one would have been motivated to have included a timer.

With respect to claim 6, wherein the verifier processor is arranged to receive pause and stop requests and is configured so that any pause and stop request is ineffective during a first check of the code (see Harding paragraph 0016).

With respect to claim 7, wherein the verifier processor can only be paused for a predetermined time (see Harding paragraph 0016).

With respect to claim 8, wherein if the application codes does not satisfy the verification function, a reset signal is asserted after a predetermined time (see Harding paragraph 0016 i.e. this may restart the validation).

With respect to claim 9, wherein a status signal is set and stored to indicate that the code does not satisfy the verification function before the reset is asserted (see Harding paragraph 0016 0018 and 0020).

With respect to claim 13, wherein the verifier processor has a stop input and is arranged to restart a given time period after a stop, and arranged not to stop again until completing the verification function on the code at least once (see Harding paragraph 0016).

With respect to claim 18, wherein impairing the function of the integrated circuit comprises resetting the circuit (see Harding paragraph 0016 i.e. this may restart the validation).

With respect to claims 23 and 29, wherein the verification processor is structured to impair the execution of the circuit by asserting a reset signal to the processor if the application codes does not satisfy the verification function (see Morais paragraph 0034-0039) within a predetermined time (see Harding paragraph 0016).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DA

Devin Almeida
Patent Examiner
5/21/2007